

bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

sending from the [a] merchant's computer over an internet network to the [a] consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

sending from said consumer's computer consumer identity and authentication information and said merchant message, to [an] the issuer gateway for an issuing bank;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description

25. (Amended) The method for electronic commerce of claim 1[, Japanese Payment Options are provided], comprising:

the issuer offering [special payment arrangements to] the consumer [,] a payment schedule conditioned on the merchant name from the merchant's digital certificate and the amount of payment from the initiation message.

26. (Amended) A system for electronic commerce, comprising:  
means for forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

[a] the merchant's computer [for] sending over an internet network to [a] the consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

a consumer's wallet program in said consumer's computer responsive to said wallet initiation message, for sending from said consumer's computer consumer identity and authentication information and said merchant message, to [an] the issuer gateway for an issuing bank;

[an] the issuer gateway [for] verifying said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

27. (Amended) A computer program product executable in a computer system, comprising:

computer program code means for forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

computer program code means for sending from [a] the merchant's computer over an internet network to [a] the consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

computer program code means for starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

computer program code means for sending from said consumer's computer consumer identity and authentication information and said merchant message, to [an] the issuer gateway for an issuing bank;

computer program code means for verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

28. (Amended) A data processing system for electronic commerce, comprising:  
means for forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

[a computer processor] means for sending from [a] the merchant's computer over an internet network to [a] the consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

means for starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

means for sending from said consumer's computer consumer identity and authentication information and said merchant message, to [an] the issuer gateway for an issuing bank;

means for verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.



33. (Amended) A method for electronic commerce, comprising:

forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

sending from [a] the merchant's computer over an internet network to [a] the consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

said acquiring bank's digital certificate containing a network address or URL that identifies the network location of said acquiring bank contacted via an internet network as part of a payment protocol;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

sending from said consumer's computer consumer identity and authentication information and said merchant message, to [an] the issuer gateway for an issuing bank;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over

said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said issuer's digital certificate containing a network address or URL that identifies the network location of the issuer contacted via an internet network as part of a payment protocol;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

34. (Amended) A method for electronic commerce, comprising:

forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

sending from [a] the consumer's computer consumer to [an] the issuer gateway for an issuing bank, an authorization request message containing consumer identity and authentication information, payment amount, an order description, a timestamp, a digital certificate representing a merchant, and a digital certificate representing [the merchant's] an acquiring bank of the merchant;

said merchant's digital certificate containing a merchant identifier unique for the acquiring bank;

[said] an acquiring bank's digital certificate containing a bank identifier unique among all banks sharing a common financial arrangement;

validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant, acquirer, and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce, said merchant identifier from the merchant's digital certificate, and said acquiring bank identifier from said acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number;

said authorization token being digitally signed by the issuing bank; and

said merchant's computer receiving said authorization token and fulfilling said order description.

Please add the following new Claims:

--46. (NEW) A method for electronic commerce, comprising:

forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;



51 C4  
amt  
B\$ sending from the merchant's computer over an internet network to the consumer's computer, a merchant message including a wallet initiation message, and a digital certificate of a merchant provided by an acquiring bank, said wallet initiation message including a payment amount, an order description, a merchant identifier and a timestamp;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

sending from said consumer's computer consumer identity and authentication information and said merchant message, to the issuer gateway for an issuing bank;

verifying at said issuer gateway that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

58  
47. (NEW) The method of Claim 46 further comprising :

providing the merchant's digital signature and matching certificate to the consumer's computer.

52

30

48. (NEW) The method of Claim 46 further comprising :

the issuer gateway signing the authorization token.

49. (NEW) A system for electronic commerce, comprising:

means for forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer;

the merchant's computer sending over an internet network to the consumer's computer, a merchant message including a wallet initiation message, and a digital certificate of a merchant provided by an acquiring bank, said wallet initiation message including a payment amount, an order description, a merchant identifier and a timestamp;

a consumer's wallet program in said consumer's computer responsive to said wallet initiation message, for sending from said consumer's computer consumer identity and authentication information and said merchant message, to the issuer gateway for an issuing bank;

the issuer gateway verifying that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that funds and/or credit are available to support the payment amount, then authorizing payment by sending over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

43

B